日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

#3

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年１２月１１日

出願番号
Application Number: 特願２０００－３７５４０６

出願人
Applicant (s): 三菱電機株式会社

２００１年 １月 ５日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２０００－３１１０２３８

【書類名】　特許願

【整理番号】　527084JP01

【提出日】　平成12年12月11日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 15/00

【発明者】

【住所又は居所】　東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

【氏名】　▲高▼本　元晴

【発明者】

【住所又は居所】　東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

【氏名】　島田　豊治

【特許出願人】

【識別番号】　000006013

【氏名又は名称】　三菱電機株式会社

【代理人】

【識別番号】　100064746

【弁理士】

【氏名又は名称】　深見　久郎

【選任した代理人】

【識別番号】　100085132

【弁理士】

【氏名又は名称】　森田　俊雄

【選任した代理人】

【識別番号】　100091409

【弁理士】

【氏名又は名称】　伊藤　英彦

【選任した代理人】

【識別番号】　100096781

【弁理士】

【氏名又は名称】　堀井　豊

【選任した代理人】

【識別番号】　100096792

【弁理士】

【氏名又は名称】　森下　八郎

【手数料の表示】

【予納台帳番号】　008693

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ログイン認証装置、およびログイン認証方法

【特許請求の範囲】

【請求項１】　イントラネットを介して端末およびウェブサーバと接続可能なログイン認証装置であって、

ユーザの識別子と、前記識別子のユーザが閲覧可能なウェブサーバ内のウェブページのアドレスと、前記識別子のユーザがその内容について変更可能なウェブページのアドレスとを記憶する記憶手段と、

前記端末から受信した識別子を前記記憶手段により記憶した識別子と照合し、前記端末から受信した識別子に対して、前記ウェブページの閲覧可否および変更可否を判断する認証手段とを含む、ログイン認証装置。

【請求項２】　前記記憶手段は、前記ユーザの識別子と、前記閲覧可能なウェブページおよび前記変更可能なウェブページとを対応付けてテーブルに記憶する、請求項１に記載のログイン認証装置。

【請求項３】　前記ログイン認証装置はさらに、

前記識別子の属性ごとに前記各ウェブページへのアクセス回数をアクセス情報として集計する集計手段を含み、

前記記憶手段は、前記アクセス情報を記憶する、請求項１または請求項２に記載のログイン認証装置。

【請求項４】　イントラネットを介して端末およびウェブサーバと接続可能なログイン認証装置を用いたログイン認証方法であって、

ユーザの識別子と、前記識別子のユーザが閲覧可能なウェブサーバ内のウェブページのアドレスと、前記識別子のユーザがその内容について変更可能なウェブページのアドレスとを記憶するステップと、

前記端末から受信した識別子を前記記憶するステップで記憶した識別子と照合し、前記端末から受信した識別子に対して、前記ウェブページの閲覧可否および変更可否を判断するステップとを含む、ログイン認証方法。

【請求項５】　前記記憶するステップは、前記ユーザの識別子と、前記閲覧可能なウェブページおよび前記変更可能なウェブページとを対応付けてテーブル

に記憶する、請求項４に記載のログイン認証方法。

【請求項６】　前記識別子の属性ごとに前記各ウェブページへのアクセス回数をアクセス情報として集計するステップをさらに含み、

前記記憶するステップは、前記アクセス情報を記憶する、請求項４または請求項５に記載のログイン認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、ログイン認証装置、およびログイン認証方法に関し、さらに詳しくは、イントラネットを介して端末およびウェブサーバと接続可能なログイン認証装置、およびログイン認証方法に関する。

【０００２】

【従来の技術】

近年情報技術の発達に伴い、企業内でイントラネットの構築がさかんに行なわれている。

【０００３】

イントラネットを構築する企業の中でも、規模の大きい企業では、たとえば、本社を中心として、各支社や各工場ごとに、または各部署ごとにウェブサーバを設置している。

【０００４】

【発明が解決しようとする課題】

これらの複数のウェブサーバは、セキュリティ確保のために、ユーザＩＤやパスワードの入力をユーザに要求する認証管理をそれぞれ独立して行なっている。そのため、ユーザが複数のウェブサーバにアクセスを繰返して業務を行なう場合に、各ウェブサーバにアクセスするたびに、各ウェブサーバごとのユーザＩＤとパスワードの入力が必要となり、ユーザにとって非常に煩雑な作業となっていた。

【０００５】

また、各ウェブサーバは複数のウェブページを有しているため、セキュリティ

補償のためウェブページ単位でも認証管理を行なう方が好ましい。しかしながらウェブサーバごとだけでなく、ウェブサーバ内のウェブページ全てについて認証管理を行なうことはユーザの操作を極めて煩雑とし、さらに、認証管理費用も増大する。よってウェブページごとの認証管理は省略せざるを得ず、ウェブサーバ単位で認証管理を行なっていた。

【０００６】

ネットワーク上での認証方法については、特開平１０－１７７５５２号公報および特開平１０－１０５５１６号公報にて提案されているが、ウェブサーバ内のウェブページ単位までセキュリティ補償を行なうものではなく、また、設定環境もイントラネットとは異なる環境である。

【０００７】

この発明の目的は、イントラネット内のウェブサーバにおいて、ウェブページ単位でセキュリティを補償し、かつユーザにとって操作が簡単であるログイン認証装置および認証方法を提供することである。

【０００８】

【課題を解決するための手段】

この発明に係るログイン認証装置は、イントラネットを介して端末およびウェブサーバと接続可能なログイン認証装置であって、ユーザの識別子と、上記識別子のユーザが閲覧可能なウェブサーバ内のウェブページのアドレスと、識別子のユーザがその内容について変更可能なウェブページのアドレスとを記憶する記憶手段と、上記端末から受信した識別子を上記記憶手段により記憶した識別子と照合し、上記端末から受信した識別子に対して、上記ウェブページの閲覧可否および変更可否を判断する認証手段とを含む。

【０００９】

好ましくはさらに、上記記憶手段は、上記ユーザの識別子と、上記閲覧可能なウェブページまたは上記変更可能なウェブページとを対応付けてテーブルに記憶する。

【００１０】

これにより、ウェブサーバ単位ではなくウェブページ単位でセキュリティの確

保が可能となり、かつ、ユーザはウェブページごとにユーザＩＤとパスワードを入力するといった煩雑な操作を行なう必要がなくなる。

【００１１】

さらに好ましくは、上記ログイン認証装置は、上記識別子の属性ごとに上記各ウェブページへのアクセス回数をアクセス情報として集計する集計手段を含み、上記記憶手段は、上記アクセス情報を記憶する。

【００１２】

これにより、ユーザに属性ごとのウェブページ利用回数を容易に確認することが可能となり、今後のウェブページの運用方針を決定するのに有効な判断要素となる。

【００１３】

この発明に係るログイン認証方法は、イントラネットを介して端末およびウェブサーバと接続可能なログイン認証装置を用いたログイン認証方法であって、ユーザの識別子と、上記識別子のユーザが閲覧可能なウェブサーバ内のウェブページのアドレスと、上記識別子のユーザがその内容について変更可能なウェブページのアドレスとを記憶するステップと、上記端末から受信した識別子を上記記憶するステップで記憶した識別子と照合し、上記端末から受信した識別子に対して、上記ウェブページの閲覧可否および変更可否を判断するステップとを含む。

【００１４】

好ましくはさらに、上記記憶するステップは、上記ユーザの識別子と、上記閲覧可能なウェブページまたは上記変更可能なウェブページとを対応付けてテーブルに記憶する。

【００１５】

これにより、ウェブサーバ単位ではなくウェブページ単位でセキュリティの確保が可能となり、しかもユーザはウェブページごとにユーザＩＤとパスワードを入力するといった煩雑な操作を行なう必要がなくなる。

【００１６】

さらに好ましくは、上記識別子の属性ごとに上記各ウェブページへのアクセス回数をアクセス情報として集計するステップをさらに含み、上記記憶するステッ

プは、上記アクセス情報を記憶する。

【００１７】

これにより、ユーザの属性ごとのウェブページ利用回数を容易に確認することが可能となり、今後のウェブページの運用方針を決定するのに有効な判断要素となる。

【００１８】

【発明の実施の形態】

以下、発明の実施の形態を図面を参照して詳しく説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【００１９】

図１はこの発明の実施の形態であるログイン認証システムの全体構成を示すブロック図である。

【００２０】

図１を参照して、企業内の各工場または各営業所である拠点イ内に設置されたログイン認証装置３００は、ファイアウォール２００、イントラネット１００を介して所外端末１０～Ｎと接続されている。

【００２１】

また、拠点イ内においてログイン認証装置３００は、所内端末１～ｎと、プロキシウェブサーバ４００とに接続されている。プロキシウェブサーバ４００はウェブページＡ１～Ａ３を有するウェブサーバＡと、ウェブページＢ１～Ｂ３を有するウェブサーバＢと、ウェブページＣ１～Ｃ３を有するウェブサーバＣとに接続可能である。なお、図１においてはプロキシウェブサーバ４００に接続可能なウェブサーバは３つとしているが、プロキシウェブサーバ４００が、３つ以上のウェブサーバと接続することも当然可能である。

【００２２】

ログイン認証装置３００は、認証部３０１と、マスタファイル３０２と、集計部３０３とを含む。

【００２３】

マスタファイル３０２は、各ウェブサーバＡ～Ｃの各ウェブページごとに接続

可能なユーザの識別子であるユーザＩＤやパスワードを表１に示すような認証テーブルとして記憶している。

【００２４】

【表１】

ユーザID	パスワード	許可コンテンツ										人事・職制情報		
		サーバA			サーバB			サーバC				工場ｺｰﾄﾞ	部ｺｰﾄﾞ	課ｺｰﾄﾞ
		A1	A2	A3	B1	B2	B3	C1	C2	C3				
A001	XX010		○	●								KUMA	AXX	100
	利用回数		126	59										
A002	AAb1	○										KUMA	BXX	200
	利用回数	15												
B003	C026		●		●	○						ITAMI	YXX	300
	利用回数		50		48	10								
B004	ax9935x3							●				FUKU	SXX	400
	利用回数							300						

【００２５】

なお、表１中の「●」印は、該当するウェブページの内容を閲覧することができるだけでなく、その内容を変更または更新することができることを示している

。また、「○」印は、該当するウェブページの内容を閲覧することはできるが、その内容を変更または更新することはできないことを示している。たとえば、表１中のユーザＩＤがＡ００１のユーザはウェブサーバＡ中のウェブページＡ２についてはその内容の閲覧はできるが、内容の変更または更新はできず、ウェブページＡ３については、その内容の閲覧だけでなく、変更または更新も可能なことを表わしている。また、それ以外のウェブページについては閲覧も変更または更新もできないことを表わしている。

【００２６】

なお、認証テーブルには、人事・職制情報として各ユーザＩＤの所属する工場コードや部コード、課コードが登録されている。

【００２７】

また、各ユーザがアクセスしたウェブページの利用回数についても表１に示すように記録される。

【００２８】

ログイン認証装置３００中の認証部３０１は、各ウェブサーバＡ～Ｃ内のウェブページへの接続を希望するユーザが使用する所外端末１０～Ｎおよび所内端末１～ｎから送信されたユーザＩＤおよびパスワードと、マスタファイル３０２中に記憶してある認証テーブル中のユーザＩＤおよびパスワードを照合し、さらに、ユーザが接続を希望するウェブページの閲覧可否、更新可否を判断する。

【００２９】

また、ログイン認証装置３００中の集計部３０３は各ユーザがウェブページにアクセスした回数をカウントし、定期的にカウントした結果を職制ごとに集計する機能を有する。

【００３０】

図２は、図１に示したログイン認証システムにおいて、ユーザが所外端末１０を用いてウェブページにアクセスする場合のログイン認証システムの動作を示すフローチャート図である。

【００３１】

図２を参照して、ユーザが所外端末１０を用いて、拠点イ内のウェブサーバＡ

内のウェブページＡ２をアクセスしたい場合、ユーザは所外端末１０にユーザＩＤおよびパスワードおよびアクセスしたいウェブページＡ２のアドレスをキーボードやマウス等の入力部（図示せず）により入力後、拠点イ内に設置されたログイン認証装置３００に向け送信する（ステップＳ１）。

【００３２】

送信されたユーザＩＤおよびパスワードおよびウェブページＡ２のアドレスはイントラネット１００を介してファイアウォール２００で受信される（ステップＳ１１）。

【００３３】

ファイアウォール２００は所外端末１０～Ｎから拠点イ内のウェブサーバＡ～Ｃへの不正なアクセスを遮断するために設けられるシステムである。ファイアウォール２００内には拠点イ内のウェブサーバＡ～Ｃにアクセス可能なユーザＩＤとパスワードが予め登録されており、ファイアウォール２００内に予め登録されているユーザＩＤおよびパスワードと、所外端末１０から送信されたユーザＩＤおよびパスワードの照合が行なわれる（ステップＳ１２）。

【００３４】

ステップＳ１２での照合の結果、ファイアウォール２００内に予め登録されたユーザＩＤおよびパスワードと、所外端末１０から送信されたユーザＩＤおよびパスワードが一致しない場合は、ファイアウォール２００は所外端末１０へ閲覧不可の通知を送信し（ステップＳ１３）、イントラネット１００を介して所外端末１０で受信される（ステップＳ２）。

【００３５】

一方、ファイアウォール２００での照合の結果、ファイアウォール２００内に予め登録されたユーザＩＤおよびパスワードと、所外端末１０から送信されたユーザＩＤおよびパスワードが一致した場合は、ファイアウォール２００はユーザＩＤとパスワードと所外端末１０で入力されたウェブページＡ２のアドレスを拠点イ内のログイン認証装置３００へ送信する（ステップＳ１２）。

【００３６】

ログイン認証装置３００は、ファイアウォール２００からユーザＩＤとパスワ

ードとウェブページＡ２のアドレスを受信後（ステップＳ２１）、受信したユーザＩＤおよびパスワードが認証テーブル上のユーザＩＤおよびパスワードと一致しているか否かを認証部３０１で確認し、さらに受信したウェブページＡ２へのアクセス希望に対して、ユーザがアクセス可能か否かを認証部３０１で確認する（ステップＳ２２）。なお確認は表１に示したマスタファイル３０２に記憶している認証テーブルを用いて行われる。

【００３７】

ここで、ユーザＩＤおよびパスワードが認証テーブル上のユーザＩＤおよびパスワードと一致していない場合は拠点イ内のウェブサーバへのアクセスはできないので閲覧不可の通知を送信する（ステップＳ２３）。送信された閲覧不可通知はファイアウォール２００を介して（ステップＳ１４）、所外端末１０で受信される（ステップＳ３）。

【００３８】

また、ユーザＩＤおよびパスワードが認証テーブル上のユーザＩＤおよびパスワードと一致していても、認証テーブル上でウェブページＡ２の閲覧が許可されていなければ、ウェブページＡ２を閲覧することはできない。

【００３９】

たとえば、所外端末１０からウェブページＡ２の閲覧を希望したユーザのユーザＩＤがＡ００１であった場合は、表１に示した認証テーブル上にて「○」印が記録されているので閲覧は可能である。しかし、ユーザＩＤがＡ００２のユーザは認証テーブル上のウェブページＡ２欄に印が記録されていないことから、ユーザＩＤがＡ００２のユーザは拠点イ内のウェブサーバには接続可能であるが、ウェブページＡ２は閲覧ができないということになる。よって、この場合においても、ユーザＩＤがＡ００２のユーザが利用している所外端末１０に対して、閲覧不可通知を送信する（ステップＳ２３）。

【００４０】

ユーザＩＤがＡ００１のユーザのように、ウェブページの閲覧が可能と認証部３０１で判断された場合は、ウェブページＡ２のアドレスがプロキシウェブサーバ４００に送信される（ステップＳ２４）。送信されたウェブページＡ２のアド

レスはプロキシウェブサーバ４００で受信され（ステップＳ３１）、プロキシウェブサーバ４００はユーザが希望するウェブページを閲覧可能な状態とする（ステップＳ３２）。

【００４１】

一方、ユーザがウェブページＡ２内の内容について変更や更新を行なう場合もある。この場合も認証部３０１でユーザがウェブページＡ２に対して変更または更新が可能か否かを判断する。たとえば、ユーザＩＤがＡ００１のユーザは表１の認証テーブルではウェブページＡ２欄に「○」印が記録されており、ウェブページＡ２について閲覧は可能であるが変更または更新はできないということになる。よって、ユーザＩＤがＡ００１のユーザが所外端末１０のキーボードやマウス等の入力部（図示せず）を用いてウェブページＡ２の内容を変更または更新しようとしたときに、更新不可通知がログイン認証装置３００からファイアウォール２００およびイントラネット１００を介して所外端末１０へ送信される（ステップＳ２３、Ｓ１４、Ｓ３）。

【００４２】

しかし、ユーザＩＤがＡ００３のユーザがウェブページＡ２の内容について変更または更新を行なう場合は、表１に示した認証テーブルのウェブページＡ２の欄に「●」印が記録してあるため、認証部３０１は照合後、ウェブページＡ２のアドレスおよびウェブページＡ２の内容の変更または更新を許可する情報をプロキシウェブサーバ４００へ送信する（ステップＳ２４）。

【００４３】

ログイン認証装置３００はプロキシウェブサーバ４００へユーザのアクセス希望ウェブページのアドレス等を送信後、ユーザの当該ウェブページの利用回数を集計部３０３でカウントする（ステップＳ２５）。カウントされた利用回数は、たとえば表１に示すように、認証テーブル上にて記録される。

【００４４】

さらに集計部３０３は表２の認証テーブルを用いて、各工場コードや部コード、課コードごとのウェブページ利用回数を集計する（ステップＳ２６）。集計結果を表２に示す。

【００４５】

【表２】

		コンテンツ利用回数								
		サーバA			サーバB			サーバC		
		A1	A2	A3	B1	B2	B3	C1	C2	C3
工場コード	KUMA	100	250	23	55	78	95	12	62	91
	ITAMI	11	50	47	…	…	…	…	…	…
	FUKU	…	…	…	…	…	…	…	…	…
	…	…	…	…	…	…	…	…	…	…
部コード	AXX	75	225	26	30	53	70	15	37	66
	BXX	…	…	…	…	…	…	…	…	…
	…	…	…	…	…	…	…	…	…	…
課コード	100	15	165	5	0	28	10	0	2	6
	200	…	…	…	…	…	…	…	…	…
	…	…	…	…	…	…	…	…	…	…

【００４６】

これにより、企業内の工場、部、または課ごとのウェブページ利用状況を容易に確認することが可能となり、利用状況に応じた各ウェブページの整理、内容の充実等を図ることが可能となる。

【００４７】

以上はユーザが所外端末１０～Ｎを用いた場合のログイン認証システムの動作を示したが、ユーザが拠点イ内の所内端末１～ｎを用いた場合についてもログイン認証システムは動作する。

【００４８】

図３はユーザが所内端末１を用いてウェブページにアクセスする場合のログイン認証システムの動作を示すフローチャート図である。

【００４９】

図３を参照して、ユーザが所内端末１を用いて、拠点イ内のウェブサーバＡ内のウェブページＡ２にアクセスしたい場合、ユーザは所内端末１にユーザＩＤおよびパスワードおよびアクセスしたいウェブページＡ２のアドレスをキーボードやマウス等の入力部（図示せず）により入力後、ログイン認証装置３００に送信する（ステップＳ１）。

【００５０】

ログイン認証装置３００は、所内端末１から送信されたユーザＩＤおよびパス

ワード、ウェブページＡ２のアドレスを受信後（ステップＳ２１）、受信したユーザＩＤおよびパスワードが認証テーブル上のユーザＩＤおよびパスワードと一致しているか否かを認証部３０１で確認し、さらにユーザがアクセスを希望するウェブページＡ２について、ユーザがアクセス可能か否かを認証部３０１で認証する（ステップＳ２２）。なお認証は表１に示したマスタファイル３０２に記憶している認証テーブルを用いて行われる。

【００５１】

認証部３０１による認証方法については、図２に示したログイン認証システムの動作と同様であるので、説明は繰返さない。

【００５２】

認証の結果、認証部３０１が所内端末１からウェブページＡ２へのアクセスを許可できないと判断した場合は、ログイン認証装置３００から閲覧不可通知を直接所内端末１へ送信し（ステップＳ２３）、所内端末１にて閲覧通知不可通知を受信する（ステップＳ２）

認証の結果、認証部３０１が所内端末１からウェブページＡ２へのアクセスを許可できる場合の動作については、図２におけるステップＳ２４以降の動作と同様であるため、その説明は繰返さない。

【００５３】

以上のようにこの実施の形態によれば、ログイン認証装置３００の設置により、ウェブページ単位でセキュリティの確保が可能となる。また、ユーザは各ウェブサーバ、各ウェブページへアクセスするたびにユーザＩＤとパスワードを入力するといった煩雑な操作から解放される。

【００５４】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと解釈されるべきである。本発明の範囲は上述した実施の形態ではなく特許請求の範囲によって定められ、特許請求の範囲と均等の意味およびその範囲内でのすべての変更が含まれることを意図するものである。

【００５５】

【発明の効果】

本発明によれば、ログイン認証装置３００のマスタファイル３０２に認証テーブルを作成し、認証テーブル上で各ユーザが閲覧や更新のできるウェブページを管理しておくことで、イントラネット内のウェブサーバにおいて、ウェブページ単位でセキュリティを補償し、かつユーザにとって操作が単純であるログイン認証装置およびログイン認証方法を提供することができる。

【図面の簡単な説明】

【図１】　この発明の実施の形態であるログイン認証システムの全体構成を示すブロック図である。

【図２】　ユーザが所外端末１０を用いてウェブページにアクセスする場合のログイン認証システムの動作を示すフローチャート図である。

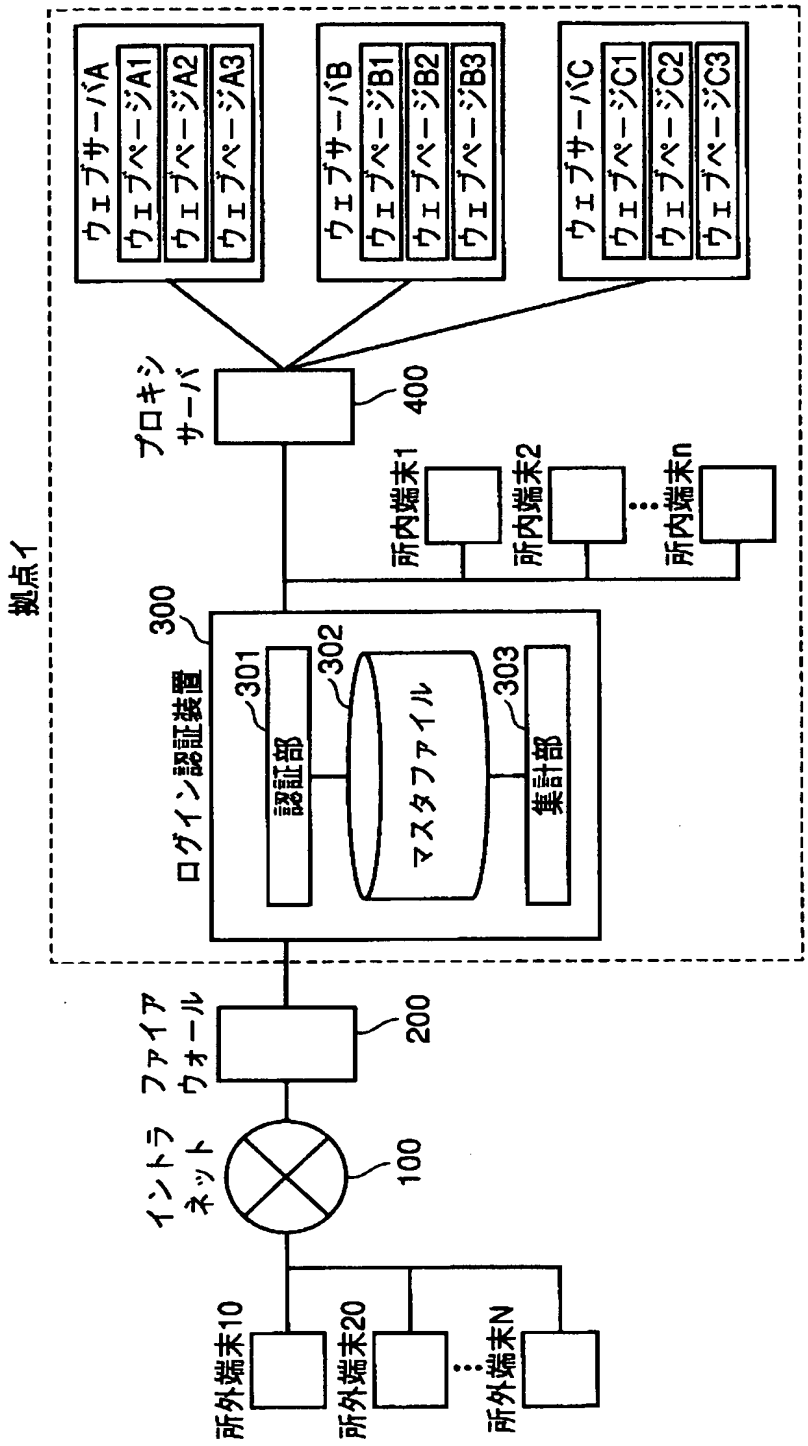
【図３】　ユーザが所内端末１を用いてウェブページにアクセスする場合のログイン認証システムの動作を示すフローチャート図である。

【符号の説明】

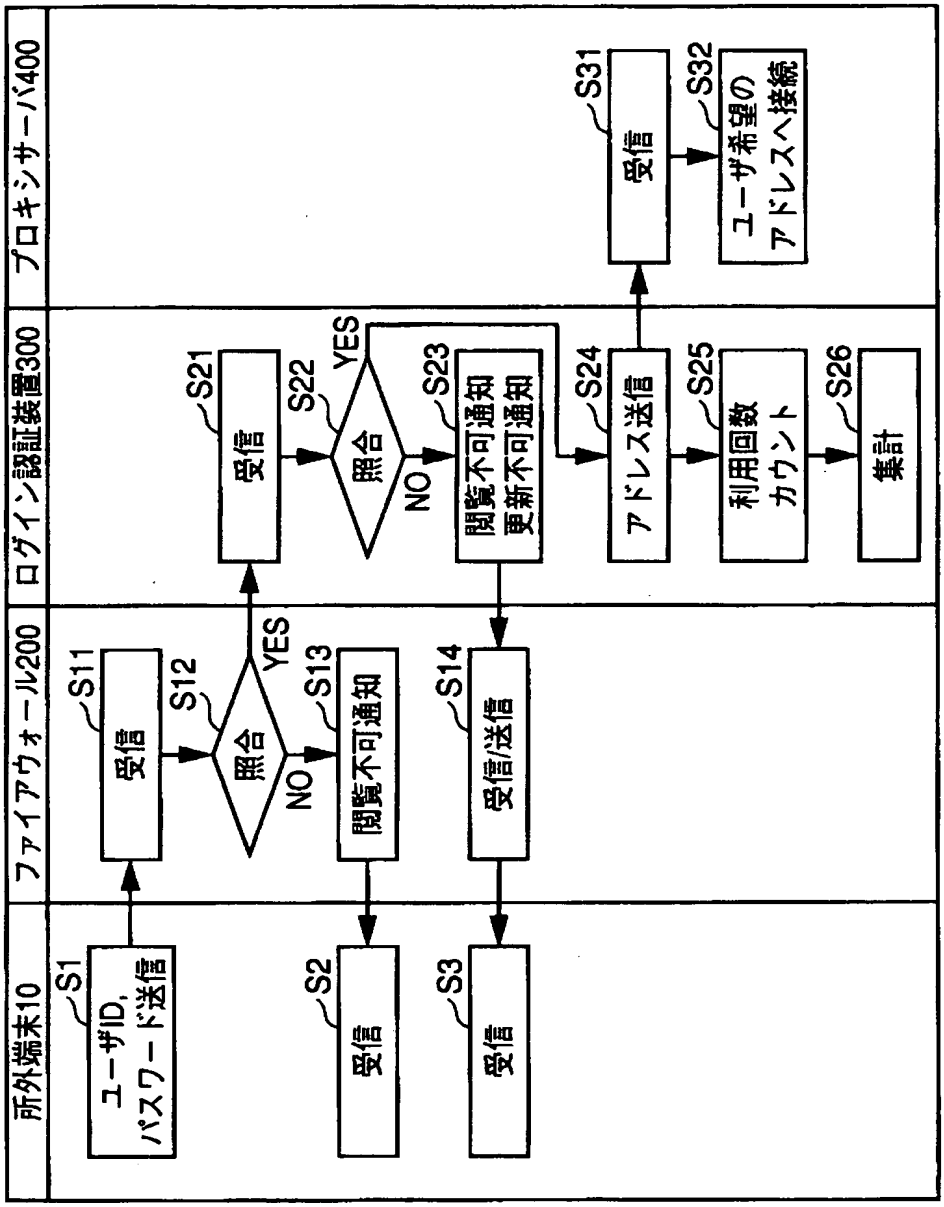
１～ｎ　所内端末、１０～Ｎ　所外端末、１００　イントラネット、２００　ファイアウォール、３００　ログイン認証装置、３０１　認証部、３０２　マスタファイル、３０３　集計部、４００　プロキシウェブサーバ。

【書類名】　　図面

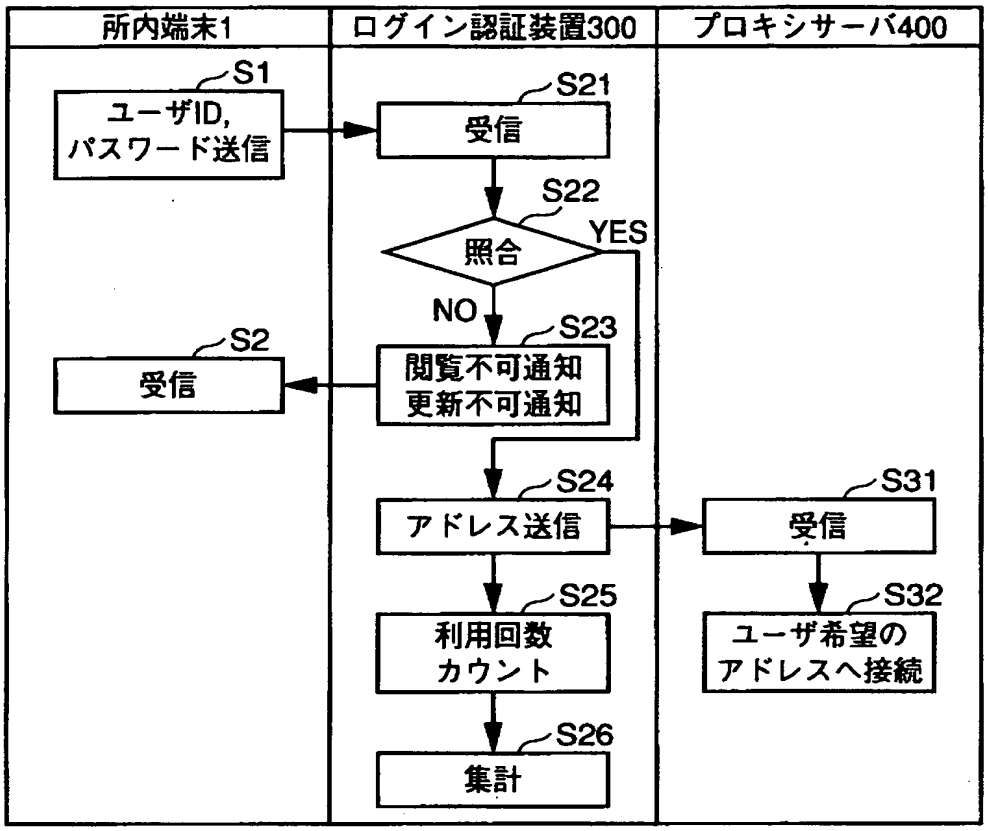
【図１】


拠点イ
ウェブサーバA
ウェブページA1
ウェブページA2
ウェブページA3
ウェブサーバB
ウェブページB1
ウェブページB2
ウェブページB3
ウェブサーバC
ウェブページC1
ウェブページC2
ウェブページC3
プロキシサーバ
400
所内端末1
所内端末2
所内端末n
300
ログイン認証装置
301
認証部
302
マスタファイル
303
集計部
ファイアウォール
200
イントラネット
100
所外端末10
所外端末20
所外端末N

【図２】


所外端末10
ファイアウォール200
ログイン認証装置300
プロキシサーバ400
S1
ユーザID,
パスワード送信
S11
受信
S12
照合
YES
NO
S13
閲覧不可通知
S2
受信
S14
受信/送信
S3
受信
S21
受信
S22
照合
YES
NO
S23
閲覧不可通知
更新不可通知
S24
アドレス送信
S25
利用回数
カウント
S26
集計
S31
受信
S32
ユーザ希望の
アドレスへ接続

【図３】


所内端末1
ログイン認証装置300
プロキシサーバ400
S1
ユーザID,
パスワード送信
S21
受信
S22
照合
YES
NO
S23
閲覧不可通知
更新不可通知
S2
受信
S24
アドレス送信
S31
受信
S25
利用回数
カウント
S32
ユーザ希望の
アドレスへ接続
S26
集計

【書類名】　　要約書

【要約】

【課題】　ウェブサーバ内のウェブページ単位でセキュリティを補償し、かつユーザにとって操作が簡単なログイン認証システムを提供する。

【解決手段】　所外端末１０または所内端末１から送信されたユーザＩＤと、パスワードと、ユーザがアクセスしたいウェブページのアドレスは、ログイン認証装置３００にて受信され、マスタファイル３０２内の認証テーブル上のユーザＩＤ等のデータと合致するか否かの認証が行われる。合致した場合は、ログイン認証装置３００はウェブページのアドレスをプロキシサーバ４００に送信し、その結果、ユーザはウェブページにアクセスすることができる。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００６０１３〕

１．変更年月日　　１９９０年　８月２４日
［変更理由］　新規登録
住　所　東京都千代田区丸の内２丁目２番３号
氏　名　三菱電機株式会社